The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PAIGE A. THOMPSON,

Defendant.

NO. CR19-159 RSL

**UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO STRIKE CRYPTOJACKING ALLEGATIONS AND TO SEVER COUNT 8**

## I. INTRODUCTION

Defendant, Paige Thompson, is charged in this case with a variety of crimes that stem from her hacking into cloud servers rented by different entities from Amazon Web Services ("AWS"). Thompson used her access to those servers, and stolen security credentials of the entities, to (1) steal data from the entities, and (2) conduct cryptocurrency mining on the servers using stolen computer power.

Thompson seeks to remove references to her cryptocurrency-mining activity from Count 1 (the overarching wire fraud count), and to sever Count 8 (which alleges the cryptocurrency mining). But there is no legal basis for Thompson's requests. Thompson's cryptocurrency-mining activity was conducted using the same attack vector as her data theft. In some cases (where a security credential had necessary permissions), Thompson used the same security credential, stolen from a victim company, to steal data from that entity, and to mine cryptocurrency on its servers. Both activities involved the same fraudulent representations that Thompson was a legitimate user of the stolen credentials, and both were designed to obtain money or property from victims (either data, or stolen computing resources).

Because the cryptocurrency mining was part and parcel of Thompson's fraud, the cryptocurrency mining allegation is directly relevant to the fraud. As a result, there is no basis for the Court to strike the allegation from Count 1. In addition, Thompson has not offered any credible argument as to why she would suffer "clear, manifest, or undue" prejudice from a joint trial. It is true that a joint trial would prevent Thompson from (falsely) portraying herself as a publicly-motivated "white hat hacker" whose intent was to help companies detect and fix security flaws. But, excluding relevant and material evidence to the contrary certainly is not a basis for severance. As a result, the Court also should deny Thompson's motion to sever.

## II. FACTS

This case arises out of Defendant, Paige Thompson's, hacking into cloud computing servers that were owned by AWS and rented by various AWS clients. Thompson used her unauthorized access to these servers and stolen security credentials to steal massive amounts of confidential information from AWS clients, and to mine cryptocurrency using stolen computing power.

### A. Amazon Web Services

AWS provides cloud-computing services to a broad variety of entities and individuals. Cloud computing is the use of remote computer servers, commonly referred to as "the cloud," rather than local computers or servers, to store, manage, and process data. AWS typically charges its cloud-computing clients on a metered, pay-as-you-go basis.

AWS clients begin with a single sign-in identity that has complete access to all AWS services and resources in the account. AWS clients then typically create Identity and Access Manager ("IAM") user accounts. IAM user accounts have either a password or an access key. IAM user accounts start with no permissions, but permissions can be added to an account by the original sign-in identity, or by an established IAM user account with permission to do so. IAM user accounts can have different permissions: for example, some may only be able to read certain data, others may be able to create new IAM user accounts, and yet others may have the ability to use the client's computing power in any manner.

IAM roles are similar to IAM user accounts, in that an IAM role has specific permissions to perform actions on AWS servers.[1] Unlike an IAM user account, an IAM role is not specific to a particular person.[2] An IAM role is meant to be assumed by any authorized IAM user that needs to perform acts permitted by the role.[3] For example, an IT manager could assign an IAM role to an employee, or software application, that needed to access a particular file directory.

Before an IAM user or application can use an IAM role, an authorized IAM user must grant permission to assume the role.[4] An IAM role does not have permanent credentials (that is, passwords or access keys) associated with it.[5] Instead, when a person assumes an IAM role, that role provides the person with a set of temporary security credentials for the role session.[6]

AWS client servers typically have one or more public-facing IP addresses. An IP address (e.g. 111.222.333.444) is a unique numeric address assigned to a computer that allows internet traffic to be sent to the computer (and that identifies the source of internet traffic sent from the computer). AWS clients' public-facing IP addresses typically are protected by firewalls. Firewalls are network security systems that monitor and control incoming and outgoing network traffic, based on predetermined security rules. To be

[1] https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
[2] *Id.*
[3] *Id.*
[4] https://aws.amazon.com/iam/faqs/ ("IAM role management");
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html
[5] https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
[6] *Id.*

effective, a firewall must be programmed, or configured, correctly. If the firewall is not configured correctly, the firewall may let traffic through, and into, the system that the person operating the firewall does not want to access the system. That traffic may include malware, that is malicious software that can operate within the system accessed.

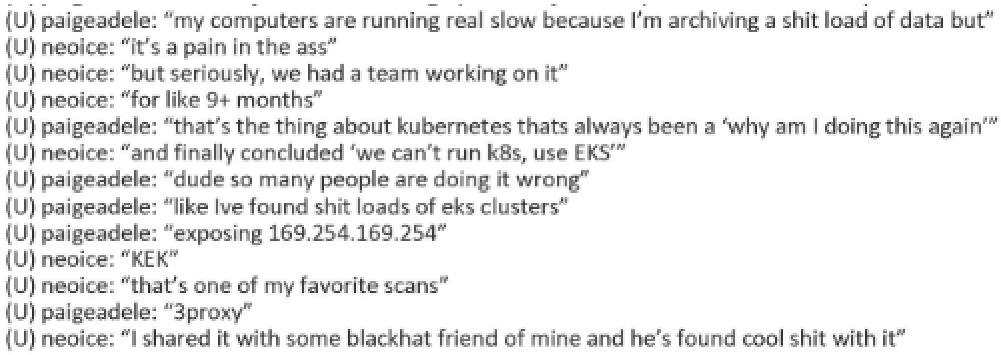
### B. Paige Thompson's Conduct

By no later than March 2019, Thompson developed a "proxy scanning" program. A proxy scanner is a computer program that scans (i.e., communicates with) large numbers of IP addresses very rapidly. Thompson designed her proxy scanner to scan the IP addresses of AWS clients, a list of IP addresses that is publicly available.

Thompson's scanner was designed to communicate with the servers that she scanned through a specific port, Port 443. A port is a number that identifies where to forward internet traffic on an internal server when the external traffic arrives. Port 443 is the standard port for secured/encrypted traffic (HTTPS). If an AWS client server was configured properly, it would recognize traffic that arrived at Port 443 as external traffic and direct it appropriately. But, a server that had not been properly configured would allow the traffic to pass though, with the result that the traffic subsequently appeared to be internal traffic. As a result, other portions of the misconfigured server – believing the traffic was internal -- would provide information and perform actions in response to commands contained in such traffic that they would not perform in response to traffic that was recognized as external.

When Thompson identified an AWS client with such a misconfiguration, Thompson communicated through Port 443 to a specific internal IP address on the client's server, 169.254.169.254 ,that is not normally accessible to external traffic. That internal address is where AWS' file system stores information about the client. Among the information stored at that internal IP address was information about IAM roles created by the client. Thompson sent commands for the internal server to provide information. These included the command "iam/info", which caused the server to provide the name of IAM role(s) created by the AWS client, as well as the command "iam/security credentials/[role]" which caused the servers to provide information including the AccessKeyId, SecretAccessKey and Token for the IAM user account.

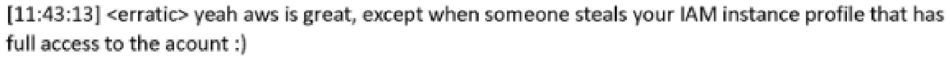
In a conversation on Slack (a business communication platform) in which she used the name "paigeadele," Thompson explained her scheme to a friend, "neoice," who commented that a "blackhat friend" used the same hack:



(U) paigeadele: "my computers are running real slow because I'm archiving a shit load of data but"
(U) neoice: "it's a pain in the ass"
(U) neoice: "but seriously, we had a team working on it"
(U) neoice: "for like 9+ months"
(U) paigeadele: "that's the thing about kubernetes thats always been a 'why am I doing this again'"
(U) neoice: "and finally concluded 'we can't run k8s, use EKS'"
(U) paigeadele: "dude so many people are doing it wrong"
(U) paigeadele: "like Ive found shit loads of eks clusters"
(U) paigeadele: "exposing 169.254.169.254"
(U) neoice: "KEK"
(U) neoice: "that's one of my favorite scans"
(U) paigeadele: "3proxy"
(U) neoice: "I shared it with some blackhat friend of mine and he's found cool shit with it"

"Blackhat" is a term that refer to hackers who break into computer networks with malicious intent.

By following this procedure, Thompson was able to identify IAM roles used by AWS clients with misconfigured firewalls (the servers of which she already was able to access). As Thompson explained in an online chat:



[11:43:13] <erratic> yeah aws is great, except when someone steals your IAM instance profile that has full access to the acount :)

Thompson exploited her access, and stolen security credentials, in multiple ways. For instance, in the case of AWS customer Capital One Financial Corporation ("Capital One"), Thompson discovered a role named ****-WAF-ROLE.[7] Capital One had assigned this role limited permissions, namely, to view certain data and to copy some of that data. As shown in computer script written by Thompson, attached as Exhibit A to this motion, Thompson assumed this role by sending a command, through Capital One's

[7] Throughout this document, the character * denotes another character that has been redacted.

misconfigured port, to “GET” the “iam/security-credentials/****-WAF-Role,” and she then used the role to issue the command “list-buckets” to Capital One’s servers. That command allowed Thompson to view the names of folders, also called buckets, of Capital One’s data.

Still using the role, Thompson then sent the command to “sync” buckets of data to her personal computer. The data that Thompson copied from Capital One included personal identifiable information (“PII”) of more than 100 million credit card applicants. Thompson similarly used stolen IAM roles of more than 30 of AWS’ other clients to steal data from those clients and to copy it to her personal computer.

With some AWS clients Thompson discovered the IAM roles that she identified had broader permissions, including, in some cases, permissions to create new virtual servers on AWS computers. A virtual server mimics the functionality of a physical server. Multiple virtual servers may be implemented on a single physical server, each with its own operating system and software.

In some instances in which Thompson identified IAM roles that had permission to create virtual servers, Thompson assumed the IAM roles and used them to send commands to create high-performance virtual servers. To AWS, these virtual servers appeared to have been created by the real AWS clients whose IAM roles Thompson had stolen. As a result, AWS allowed the servers to operate, and billed the legitimate AWS clients for the servers’ use.

After establishing these servers, Thompson placed malware on them. The malware “mined” cryptocurrency, specifically, Ethereum. Mining cryptocurrency is the process by which cryptocurrency transactions are verified and added to a public ledger, known as the blockchain. Persons who verify transactions are referred to as “miners” and are rewarded with payments of cryptocurrency.

Mining operations consume large amounts of electricity. But, because Thompson had assumed AWS clients’ roles to create the virtual servers to mine cryptocurrency, the AWS clients and/or AWS bore the cost of the mining, while Thompson personally received the payments. (What Thompson did is commonly referred to as "cryptojacking," because it involves highjacking someone else's resources to mine cryptocurrency for one's own benefit.) Thompson also wrote code to erase the evidence of her cryptocurrency malware from victim computer logs.

In some cases, where IAM roles had appropriate permissions, Thompson used the same stolen IAM roles both (i) to steal data from AWS clients and (2) to cryptojack from those clients. For instance, as set forth in the Superseding Indictment, Thompson used her unauthorized access to servers rented by, and IAM roles of, Victim 7 and Victim 8 to steal their data. *See* Dkt. No. 102, Count 1, ¶ 20. Thompson used those same IAM roles to conduct cryptojacking on AWS servers rented by Victim 7 and Victim 8 (and other victims). *See id.* Count 8.

Thompson engaged in this scheme from March 2019 until her arrest in late July 2019 (and, even after her arrest, cryptocurrency miners that she previously had deployed continued their mining activity into early August 2019).

### C. **Procedure**

Thompson currently is charged in a Superseding Indictment, returned by the grand jury on June 17, 2021. Count 1 of that Superseding Indictment charges Thompson with a wire fraud scheme. That count alleges that Thompson exploited a misconfiguration in AWS customers' firewalls to obtain those customers' security credentials, and then used those credentials to steal information from the customers. It also alleges that Thompson used her unauthorized access to mine cryptocurrency on some of the same AWS customers' servers. (Although the identities of some of the victims have been anonymized in the public document, the government has identified the victims to Thompson.)

Counts 2 through 7 of the Indictment each alleges a specific violation of 18 U.S.C § 1030(a)(2) in which Thompson accessed a particular AWS client's servers without authorization and obtained information from the servers. Each count identifies the AWS client and the date of the intrusion. Count 8 alleges that Thompson violated 18 U.S.C

§ 1030(a)(5) by accessing AWS customers' servers (including customers identified in Counts 2-7) and using her unauthorized access to mine cryptocurrency. Count 9 alleges that Thompson committed access device fraud, in violation of 18 U.S.C § 1029, by possessing information stolen during the course of Count 1 with the intent to create counterfeit and unauthorized credit and debit cards to be used to commit fraud. And Count 10 alleges that Thompson committed aggravated identity theft in violation of 18 U.S.C § 1028A.

The government currently plans to present a Second Superseding Indictment to the grand jury during the first half of January 2022. The Second Superseding Indictment does not add any additional charges, but rather clarifies facts underlying certain of the current charges, consistent with the factual recitation set forth above. A copy of the proposed Second Superseding Indictment is attached as Exhibit B. Assuming that the grand jury returns a true bill, the Second Superseding Indictment will be the operative charging document by January 14, 2022, when Thompson's motions are fully briefed and the Court considers the motions.

## III. ARGUMENT

### A. The Court Should Not Strike the Cryptojacking Allegations from Count 1

Thompson asks that the Court strike from Count 1 the allegation that she engaged in cryptojacking. The Court should deny this request because the cryptojacking allegation is one of the two ways in which Thompson committed wire fraud, as alleged in Count 1.

Federal Rule of Criminal Procedure 7(d) provides that, "[u]pon the defendant's motion, the court may strike surplusage from the indictment or information." Fed. R. Crim. P. 7(d). "The purpose of a motion to strike under Fed. R. Crim. P. 7(d) is to protect a defendant against 'prejudicial or inflammatory allegations that are neither relevant nor material to the charges.'" *United States v. Terrigno*, 838 F.3dd 371, 373 (9th Cir. 1988) (quoting *United States v. Ramirez*, 710 F.2d 535, 544-45 (9th Cir. 1983)).

A motion to strike surplusage from an indictment should not be granted "unless it is clear that the allegations are not relevant to the charge and are inflammatory and prejudicial." Charles A. Wright & Andrew D. Leipold, Federal Practice and Procedure § 128, Amendment of Indictments; Surplusage (4th ed.). This "is an exacting standard." *Id.* And, in fact, courts consistently deny motions to strike where the material that the defendant seeks to strike is relevant. *See, e.g.*, *United States v. Laurienti*, 611 F.3d 530, 547 (9th Cir. 2010) (affirming denial of motion to strike word "unlawful" used to describe certain payments, because the government sought to prove that the payments were unlawful and it was relevant that they were); *Terrigno*, 838 F.3d at 373-74 (affirming denial of motion to strike various statements, including statement that money embezzled was intended for the poor and homeless, because statement was "relevant and material" to the charge of embezzlement); *United States v. Hedgepath*, 434 F.3d 609, 612 (3d Cir. 2006).

Applying these standards, the Court should not strike the cryptojacking allegation from Count 1. As described in Part II above, and laid out in Count 1 of the Superseding Indictment, and even more clearly in Count 1 of the planned Second Superseding Indictment, between March and early August of 2019, Thompson engaged in a scheme to defraud AWS customers and AWS in two separate ways, that had a common nucleus of fact.

Thompson used a proxy scanner to identify AWS customers with misconfigured firewalls. Thompson took advantage of the misconfiguration to steal information about IAM roles that the customers had established. Thompson then assumed those roles and used them to issue commands to the customers' servers. Depending upon what permission the roles had, these could be commands to steal customer data and copy it to Thompson's computer. And they could be commands to create new virtual servers and use them to mine cryptocurrency for Thompson's personal benefit. In the case of customers' whose IAM roles had permissions that allowed Thompson to do both – such as Victim 7 and Victim 8 – Thompson did both.

In both cases, Thompson engaged in the same fraud and deceit and she made the same implicit false representations: namely, that the commands that she issued using the roles and security credentials that she had stolen were legitimate commands sent by users with permission to send such commands, rather than commands sent by a person who had stolen the security credentials and lacked the authority to use the roles. And, in both cases, Thompson did so to obtain money or property. In the case of her data theft, she did so to obtain the information that she stole. *See Carpenter v. United States,* 484 U.S. 19, 25-26 (1987) (holding that information can constitute property for purposes of the federal fraud statutes). In the case of the cryptomining, she did so to obtain the free use of computing resources.

Thompson's motion attempts to distinguish between the government's two theories by arguing that the government does not allege that Thompson attempted to profit from her data theft, and suggests that fact renders the cryptocurrency mining allegation particularly inflammatory. Thompson's argument is factually incorrect. Count 9 of the indictment alleges that Thompson possessed stolen information with the intent to defraud, including by obtaining counterfeit credit or debit cards. *United States v. Berger*, 473 F.3d 1080, 1103 (9th Cir. 2007) (indictments are to read as a whole). At trial, the government will introduce evidence that Thompson appears to have taken steps in this direction. Given this fact, Thompson's actual cryptocurrency mining is not particularly inflammatory or confusing.

But, even if it were, the court cannot strike the allegation. It is not merely relevant – it is central to the government's theory. Therefore, the Court should not strike the allegations concerning cryptocurrency mining from Count 1. *See, e.g.*, *Terrigno*, 838 F.3d at 373 (Rule 7(c) is designed to apply only if statements are not relevant). (To the extent that what Thompson is seeking is actually a severance, the Court also should not grant that relief, for the reasons set forth in Part III.B.)

## B. The Court Should Not Sever Count 8

Thompson also asks the Court to sever Count 8 from the other charges in this case. The Court also should deny this motion.

### *1. Count 8 is Properly Joined*

Federal Rule of Criminal Procedure 8(a) governs joinder of offenses. Multiple offenses may be joined if they are (1) "of the same or similar character," (2) "based on the same act or transaction," or (3) "connected with or constitute parts of a common scheme or plan." Fed. R. Crim. P. 8(a). The validity of joinder is determined on the basis of the allegations contained within the four corners of the indictment. *See United States v. Jawara*, 474 F.3d 565, 572 (9th Cir. 2007).

"Rule 8 is to be broadly construed in favor of initial joinder." *United States v. Friedman*, 445 F.2d 1076, 1082 (9th Cir. 1971). In essence, Rule 8 encourages joinder of counts when they are "logically related, and there is a large area of overlapping proof." *United States v. Anderson*, 642 F.2d 281, 284 (9th Cir. 1981). This permissive approach best serves the interests the Rule is designed to promote. Consolidating offenses that arise from the same or related acts conserves judicial resources, minimizes inconvenience to witnesses, and avoids unnecessary delays in bringing a defendant to trial. *See United States v. Lane*, 474 U.S. 438, 449 (1986). Joinder also permits the trier of fact to see and consider "the complete set of facts about the alleged criminal enterprise." *See United States v. Singer*, 782 F.3d 270, 277 (6th Cir. 2015) (citing 1A Charles A. Wright & Andrew D. Leipold, Federal Practice and Procedure § 143, at 35-40 (4th ed. 2008)).

Applying these standards, Count 8, which alleges damage to protected computers based upon Thompson's cryptocurrency mining, is properly joined with the other counts in this case. In fact, Thompson's case satisfies all three prongs of Rule 8. The two offenses are of a same or similar character, because both involve hacking into AWS customers' servers through the same attack vector. They are based on the same acts and transactions, since they involve the use of the same proxy scanner to find firewall misconfigurations and steal security credentials, and, because in at least some cases (where the stolen credentials had appropriate permissions), Thompson stole data from, and planted cryptocurrency mining software on, servers of the same victims. And, they constitute parts of a common scheme or plan to breach AWS customers' servers for Thompson's own benefit.

For all of these reasons, the Court should find that Count 8 is properly joined with other charges in this case.

2. *The Court Should Not Sever Count 8*

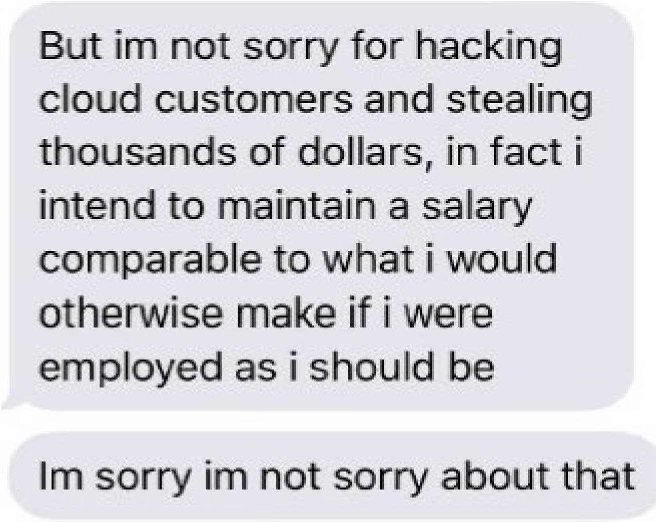
Even if joinder is appropriate, Federal Rule of Criminal Procedure 14(a) permits a district court to "order separate trials of counts" "[i]f the joinder of offenses in an indictment . . . appears to prejudice a defendant." The standard necessary to invoke Rule 14, however, is "exacting." *Jawara*, 474 F.3d at 579. The defendant bears the burden to demonstrate "clear, manifest or undue" prejudice of such magnitude that, without severance, the party's right to a fair trial will be denied. *United States v. Vasquez-Velasco*, 15 F.3d 833, 845-46 (9th Cir. 1994) (internal quotations and citations omitted); *United States v. Lewis*, 787 F.2d 1318, 1321 (9th Cir. 1986) (Under Rule 14, "[t]he defendant has the burden of proving that the joint trial was manifestly prejudicial," such that "defendant's right to a fair trial was abridged")

Significantly, too, nothing in Rule 14 requires that severance be the sole remedy. Instead, "less dramatic measures, such as limiting instructions, often will suffice to cure any risk of prejudice" from joinder. *United States v. Zafiro*, 506 U.S. 534, 539 (1993) (holding that Rule 14 leaves the tailoring of appropriate relief to the sound discretion of the trial court). In sum, joinder is the rule rather than the exception, and a trial court's determination that joinder is appropriate will be given deference, absent a showing that "joinder was so manifestly prejudicial that it outweighed the dominant concern with judicial economy and compelled exercise of the court's discretion to sever." *United States v. Armstrong,* 621 F.2d 951, 954 (9th Cir. 1980).

Thompson claims that the court should sever Count 8, because joinder supposedly would "impermissibly confuse the jury" and thereby prejudice her. *See* Defendant's Mot.

at 8. This argument fails for multiple reasons. First, Thompson does not provide any explanation of why this evidence would be so confusing, because there is none. There is no reason that evidence concerning cryptocurrency mining would be any more confusing than any other evidence in this technical case. Indeed, it likely would be less confusing, given popular interest in cryptocurrency. Second, to the extent that Thompson has any concern about spillover, the court will instruct the jury to consider evidence as to each count separately, and there is no reason to presume the jury will not follow that instruction. *See Richardson v. Marsh*, 481 U.S. 200, 211 (1987) (juries are presumed to follow instructions).

Third, a severance of Count 8 would not serve any purpose. Even if the count were severed, evidence of Thompson's cryptocurrency mining would be admissible at Thompson's trial on the remaining counts. For example, Thompson bragged on social media and in text and chat communications that she made thousands of dollars from hacking and cryptojacking AWS's cloud computing customers:



But im not sorry for hacking cloud customers and stealing thousands of dollars, in fact i intend to maintain a salary comparable to what i would otherwise make if i were employed as i should be

Im sorry im not sorry about that

Evidence that she, in fact, was doing so is important evidence that will be admissible to help prove that Thompson was the person who intentionally hacked into AWS customers' servers and stole data from them. (Thompson also bragged about her data theft, with the result that evidence of those crimes would be admissible at Thompson's trial on a severed Count 8.) As a result, severance would not avoid the prejudice Thompson asserts.

Thompson complains that the indictment provides less detail about her cryptocurrency mining than it does concerning her other crimes. There is a reason for this. As explained by the government to Thompson's counsel during the government's initial presentation about the case, Thompson designed her cryptocurrency mining activity to be hard to detect. Among other things, her software deleted itself from victims' servers (and then ran from active memory), and it deleted logs on the servers that would show its existence. *See* United States' Opposition to Defendant's Motion to Dismiss Counts 1, 9, and 10 of the Superseding Indictment, Exhibit A, at 33 (Dkt. 132) (filed under seal). As a result, Thompson's cryptocurrency mining activity left fewer forensic traces than her data theft. This explains why the charging language of Count 8 is broader. But, it is not a reason to sever the count.

Finally, Thompson argues that Count 8 should be severed because Counts 2-7 charge that Thompson accessed a computer without authorization, but Count 8 does not contain this language. There is no basis for this argument. The reason that Count 8 does not contain the language is that 18 U.S.C § 1030(a)(5), under which the count is charged, contains different statutory language, and elements, than 18 U.S.C § 1030(a)(2). Count 8 does contain the allegation, consistent with the statute and elements for that count, that Thompson "caused damage without authorization." The fact that the lack of authorization relates to damage, as opposed to access, is scarcely a reason to sever Count 8 (particularly where the obvious reality is that Thompson also did not have authorized access to conduct her cryptocurrency mining).

In sum, Thompson has not offered any credible basis for the Court to sever Count 8 from the other charges in this case. Nothing about joinder is unduly prejudicial. It simply prevents Thompson from falsely portraying herself at trial as a public-spirited white hat hacker. As a result, the Court should decline to sever Count 8.

## IV. CONCLUSION

For the foregoing reasons, the Court should deny Thompson's motion.

DATED: December 23, 2021.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

*/s Andrew Friedman*
*/s Jessica M. Manca*
ANDREW FRIEDMAN
JESSICA M. MANCA
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Telephone: (206) 553-7970
Fax: (206) 553-0882
E-mail: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdoj.gov